LA CONFIDENTIALITÉ DANS LES FUSIONS ET ACQUISITIONS ET L'IMPORTANCE DE LA PROTECTION DES DONNÉES

Publié le 6 avril, 2023

Catégories: Perspectives, Publications

En 2006, le mathématicien britannique Clive Humbly a fait cette déclaration rendue célèbre : « Les données sont le nouveau pétrole ». En effet, cette ressource gagne en valeur dans un nombre grandissant de secteurs. C'est pourquoi il est capital, avant de procéder à une opération de fusion et acquisition, d'évaluer les mesures de protection en place dans la société visée.

Comme il a déjà été dit, une foule de problèmes de confidentialité peuvent nuire à cette opération. Par exemple, une société qui ne respecte pas la Loi canadienne anti-pourriel[1], est passible de lourdes amendes, et la mauvaise gestion des consentements peut rendre de vastes quantités de renseignements personnels pratiquement inutilisables. Sans compter que les refontes du régime canadien de protection de la vie privée en cours et à venir (avec leurs sévères sanctions) sont loin de réduire les coûts de la mise à niveau des programmes de sécurité d'une société.

Cela dit, au chapitre de la confidentialité, il n'y a pas de danger plus grand pour une opération qu'une **atteinte à la sécurité des données**. Ce type d'atteinte peut créer des obligations relatives aux avis réglementaires et à la communication, donner lieu à des actions collectives, ternir une réputation et engendrer des sanctions réglementaires. Même si l'atteinte ne porte pas sur des renseignements personnels, elle peut viser des éléments de propriété intellectuelle ou d'autres renseignements confidentiels, ou perturber les activités de la société.

Les prochaines lignes portent sur l'importance de la protection diligente des données et présentent des conseils pour bien réussir ce processus, et des stratégies d'atténuation pour conclure une entente avec une société à risque. Nous verrons aussi la nécessité de repérer et de corriger rapidement toute lacune dans le programme de sécurité d'une société acquise.

Exemples récents d'atteinte à la sécurité des données dans le cadre d'opérations commerciales

Les atteintes à la sécurité des données, qu'elles soient découvertes pendant ou après l'opération, peuvent avoir de graves conséquences sur l'entente et les sociétés concernées.

Par exemple, en 2016, deux atteintes repérées avant l'acquisition de Yahoo par Verizon ont obligé les vendeurs à baisser leur prix de 350 M $ US[2].

De même, dans ses *Conclusions en vertu de la LPRPDE n° 2022-005*, le Commissariat à la protection de la vie privée du Canada (CPVP) explique avoir enquêté sur l'acheteur pour son défaut de prendre des mesures d'atténuation à l'égard d'une atteinte qui avait déjà touché les systèmes de la société cible avant la conclusion de l'opération. En 2014, un attaquant a réussi à introduire des logiciels malveillants dans le système informatique de la société. Au moment de l'opération, en 2016, l'acheteur et la cible ignoraient tous les deux que la base de données de la cible avait été compromise. La compromission n'a été découverte qu'en 2018, alors que les attaquants avaient déjà téléchargé quelque 339 millions de dossiers de cette base.

L'acheteur a alors fait l'objet d'une enquête de l'Information Commissioner's Office du Royaume-Uni (ICO) et du CPVP, au terme de laquelle l'ICO a annoncé son intention d'imposer à l'acheteur une amende de 99 M€ (somme qui a ensuite été réduite à 18,4 M€). L'enquête de l'ICO a révélé que l'acheteur n'avait pas effectué une vérification diligente au moment de l'achat et aurait dû en faire plus pour protéger ses systèmes[3].

Le CPVP a quant à lui publié son rapport d'enquête en septembre 2022, qui reprenait largement les constats de l'ICO. Plus précisément, le CPVP a trouvé que l'acheteur aurait pu détecter l'atteinte plus tôt et en réduire les conséquences s'il avait : (i) mis en place des mesures plus complètes de journalisation et de surveillance, (ii) appliqué adéquatement ses contrôles d'accès à l'authentification multifactorielle, et (iii) mis en place des mesures de responsabilisation adéquates pour assurer l'évaluation et la révision continues de ses mesures de sécurité.

Diligence en matière de sécurité des données

Pour atténuer les risques associés aux atteintes à la sécurité des données, les acheteurs doivent évaluer la sécurité de ces données dans le cadre de leur stratégie de vérification diligente, surtout si les données forment un élément important de l'opération ou si des renseignements personnels délicats sont régulièrement recueillis par la société visée. Les acheteurs devraient notamment envisager de demander les éléments suivants à la société cible :

- une copie des politiques sur la sécurité des données, y compris les plans de sécurité technique, les procédures de sauvegarde et les plans d'intervention en cas d'atteinte;
- de l'information sur les types de renseignements personnels recueillis, et si des politiques sur la conservation et la suppression des données sont en vigueur;
- de l'information sur la gestion du personnel, comme la vérification des antécédents, la conclusion d'ententes de confidentialité ou la tenue de formations sur la cybersécurité;

- de l'information sur la façon dont la société traite les tiers, comme l'évaluation de la posture de sécurité des fournisseurs de service ou des entreprises liées qui traitent des données pour la société;
- de l'information sur les vérifications de protection de la vie privée et de cybersécurité (internes et externes), y compris leur fréquence et des exemplaires des rapports récents;
- de l'information sur les atteintes passées (et les mesures prises pour y remédier);
- une copie des polices d'assurance relative à la cybersécurité, le cas échéant, et de l'information sur les réclamations passées.

Quand le volume ou le degré de confidentialité des données traitées sont particulièrement élevés, l'acheteur doit penser à retenir les services d'experts en technologies de l'information (internes ou externes) pour évaluer les mécanismes de contrôle de la sécurité en place.

Il est crucial de faire appel à des conseillers externes d'expérience pour déterminer les lacunes qui devraient sonner l'alarme et celles qui réduisent la valeur de la société.

Stratégies d'atténuation

Disons que vous découvrez un grave problème de sécurité des données chez la société visée par votre opération. Faut-il tout laisser tomber?

Dans la plupart des cas, selon la tolérance au risque de l'acheteur, les faiblesses du programme de sécurité de la société ne feront pas nécessairement avorter votre projet. L'acheteur a plusieurs options pour atténuer les risques. Par exemple :

i. négocier une indemnité pour les pénalités ou les frais de litiges associés à toute atteinte survenue avant la conclusion de l'opération ou dans une période raisonnable après;
ii. négocier une réduction du prix pour tenir compte du risque d'incident lié à la sécurité des données;
iii. négocier une retenue ou un dépôt;
iv. négocier, dans le contrat d'achat, l'obligation pour la société acquise de corriger son programme de sécurité des données avant ou immédiatement après l'opération.

Certains acheteurs pourraient chercher une assurance déclarations et garanties pour se protéger contre ce type de risque. Toutefois, ce n'est pas toujours une façon viable de gérer les problèmes de sécurité, surtout quand le problème est connu. Les assureurs connaissent les conséquences d'une atteinte à la sécurité des données et limitent souvent, voire excluent complètement la gestion de la sécurité des données de leurs polices d'assurance déclarations et garanties.

Dans le cas contraire, ils exigent maintenant que la société visée respecte des seuils minimaux de contrôles, définis au terme d'une vérification diligente complète par l'acheteur.

Points à retenir

- L'acheteur d'une société peut être tenu responsable d'atteintes à la sécurité des données antérieure à l'acquisition.
- Les logiciels malveillants peuvent rester longtemps cachés dans le système d'une entreprise.
- À l'étape de la vérification diligente raisonnable d'une opération, il faut faire appel aux tiers appropriés (y compris un conseiller juridique d'expérience et des professionnels de la sécurité des technologies de l'information, au besoin) pour vérifier la conformité des systèmes de sécurité de la société visée, selon le volume et le degré de confidentialité des données sous sa garde ou son contrôle.
- Les risques à l'opération peuvent être atténués grâce à diverses techniques de négociation ou par la souscription d'une assurance déclarations et garanties (mais ce type de police ne suffit pas toujours).
- Après l'opération, il est essentiel de faire l'inventaire de toutes les données sous la garde de la société pour bien les protéger.

[1] *Loi visant à promouvoir l'efficacité et la capacité d'adaptation de l'économie canadienne par la réglementation de certaines pratiques qui découragent l'exercice des activités commerciales par voie électronique et modifiant la Loi sur le Conseil de la radiodiffusion et des télécommunications canadiennes, la Loi sur la concurrence, la Loi sur la protection des renseignements personnels et les documents électroniques et la Loi sur les télécommunications*, L.C. 2010, ch. 23, aussi appelée communément la Loi canadienne anti-pourriel.

[2] Wall Street Journal, *Why Verizon Decided to Stick With Yahoo Deal After Big Data Breaches* (juillet 2017). En ligne. Le prix d'achat définitif s'est élevé à 4,48 G$ US.

[3] ICO du Royaume-Uni, no d'enquête : COM0804337 (octobre 2020), En ligne.

par Robbie Grant, Mitch Koczerginski, Adriana Rudensky et Christopher J. Garrah

Mise en garde